JPEE 실천공학교육논문지
JOURNAL OF PRACTICAL ENGINEERING EDUCATION

산학연계교육 분과
J. Pract. Eng. Educ. 15(3), 641-647, 2023

어깨 너머 공격을 차단하고 사용 편의성이 가능한 개선된 그룹 키패드 설계

Design of an Enhanced Group Keypad to Prevent Shoulder-Surfing Attacks and Enable User Convenience

문형진*

성결대학교 정보통신공학과

Hyung-Jin Mun*

Department of Information & Communication Engineering, Sungkyul University, Anyang 14097, Korea

[요 약]

핀테크 환경에서 스마트 폰을 이용한 금융거래가 안전하게 거래되기 위해서는 스마트 폰의 소유자에 대한 인증이 필수적이다. 스마트 폰을 이용한 인증기법은 패스워드 인증, 생체인증, SMS 인증 등이 있다. 사용자 인증에서 패스워드 입력을 통한 인증이 보편적이고 편리성이 높기 때문에 스마트 폰에서 많이 활용되고 있다. 손쉬운 인증이지만 키로깅 공격이나 엿보기 등의 공격에 취약점이 존재한다. 스마트 폰에서 패스워드 입력에서의 취약점을 해결하기 위한 보안 키패드가 제안되고 있다. 터치하는 위치로 입력하는 문자를 유추하는 공격에 강인한 그룹 키패드가 제안되었지만 사용 편리성 측면에 개선이 필요하다. 본 연구에서는 기존의 그룹 키패드에서 그룹핑된 키패드를 측면에 배치하고, 드래그를 활용하여 편리성을 제공하면서 엿보기나 레코딩 공격에 강한 새로운 방법을 제안하고자 한다. 제안 기법은 레코딩 공격을 차단하기 위해 마지막 문자확인 대신 키패드의 새로운 표시를 통해 사용자가 쉽게 확인하고, 터치하는 방법에서도 드래그를 사용하였다. 국내 사용자를 위한 다양한 배치 방법을 제시하여 패스워드 입력에서 기존 방식보다 입력의 효율성과 안전성을 제시하였다.

[Abstract]

In the fintech environment, ensuring secure financial transactions with smartphones requires authenticating the device owner. Smartphone authentication techniques encompass a variety of approaches, such as passwords, biometrics, SMS authentication, and more. Among these, password-based authentication is commonly used and highly convenient for user authentication. Although it is a simple authentication mechanism, it is susceptible to eavesdropping and keylogging attacks, alongside other threats. Security keypads have been proposed to address vulnerabilities in password input on smartphones. One such innovation is a group keypad, resistant to attacks that guess characters based on touch location. However, improvements are needed for user convenience. In this study, we aim to propose a method that enhances convenience while being resistant to eavesdropping and recording attacks on the existing group keypad. The proposed method uses new signs to allow users to verify instead of the last character confirmation easily and employs dragging-to-touch for blocking recording attacks. We suggest diverse positioning methods tailored for domestic users, improving efficiency and security in password input compared to existing methods.

Key Words: Secure Keypads, Grouping Pads, Shoulder Surfing Attack, Virtual Keypads, Password, Double touch, Recording Attack

http://dx.doi.org/10.14702/JPEE.2023.641

Received 30 October 2023; **Revised** 22 November 2023
Accepted 5 December 2023

***Corresponding Author**
E-mail: jinmun@gmail.com

I. 서 론

스마트 폰의 발전과 급격한 보급으로 다양한 서비스가 보편화되고, 개인별 서비스를 위해 소유자 여부를 확인할 수 있는 인증기술이 요구된다. 핀테크 기술을 활용한 금융거래와 같은 서비스를 이용할 때 스마트 폰이 가지는 취약점이 존재한다[1].

PC환경에서 가능한 공격들이 스마트 폰으로 이전되면서 치명적인 공격이 되고 있다. 특히, 스마트 폰에서의 금융 거래의 활성화로 PC에서 이루어진 공격이 모바일 단말기에서도 가능하다[2-4]. 스마트 폰을 이용한 SNS나 수신받은 SMS를 이용하여 피싱이나 스미싱, 어깨너머 공격(Shoulder surfing attack)과 같은 사회공학기법 공격이 이루어지고 있다[3,5,6]. 사회적공학기법을 이용한 악성코드나 불법 파일로 인한 멜웨어 설치, 키로깅과 같은 다양한 공격을 차단하기 위한 연구들이 진행되고 있다[7].

사용자가 스마트 폰에서 터치하는 것을 몰래 엿보는 행위를 훔쳐보기 공격 또는 어깨너머 공격이라고 한다. 뿐만 아니라 스마트 폰의 고해상도 촬영이 가능한 카메라가 내장되어 공격자의 폰으로 사용자의 입력하는 과정을 촬영하거나 입력하는 것을 엿보면서 입력된 패스워드 등을 훔쳐볼 수 있다[6,8].

따라서 스마트 폰에서 비밀정보를 안전하게 입력할 수 있는 보안 키패드가 요구된다. 스마트 폰의 터치 화면이 작기 때문에 다음과 같은 다양한 취약점을 가지고 있다.

- 스마트 폰의 터치영역에 모든 영문자와 숫자를 보여주기 위해서는 키패드의 크기가 상대적으로 작아진다.
- 작은 화면에 보여지는 작은 키패드의 크기로 인해 사용자가 입력할 때 실수가 발생한다.
- 훔쳐보기 등의 공격이나 악성코드 등으로 터치 위치 노출 시 입력된 패스워드 유추 가능성이 존재한다.
- 터치 위치나 훔쳐보기로 인한 공격을 회피하기 위해서는 키패드 사이의 여백이 필요하다.

스마트 폰이 가지는 취약점인 작은 스크린으로 인해 발생하는 문제를 해결하기 위한 방안이 모색되고 있다. 테트리스 모양의 키패드를 적용할 경우 테트리스의 특징으로 결합되는 부분이 많을 경우, 더 많은 여백을 확보할 수 있지만 기존 키패드보다 크기가 작아지는 단점이 있어 터치에 어려움이 존재한다. 작은 스크린에 보여지는 문자의 수를 줄이면 키패드의 크기를 커지므로 대안이 될 수 있다. 패스워드로 사용가능한 모든 문자를 그룹핑을 하여 그룹을 제시하고, 선택된 그룹의 키패드를 보여주는 방식이 제안되었다. 하지만 하나의 문자를 입력하기 위해서 키패드를 2번 터치해야 하는 번거러움과 원하는 문자가 속한 그룹을 선택해야 하는 문제가 있다.

본 연구에서는 이런 문제를 해결하기 위해 개선된 그룹핑 보안 키패드를 제안하고자 한다. 이는 그룹 키패드의 단점을 해결하고 훔쳐보기나 마지막 입력확인의 취약점을 해결할 수 있는 개선된 기법이다. 터치의 효율성을 제고하면서 개선된 보안 키패드는 다음과 같은 요구사항이 요구된다.

- 기존 방식은 매번 그룹핑 키패드 선택 후 내부 키패드 선택 시 번거러움을 최소화해야 한다.
- 키패드의 배치는 사용자의 입력 편리성을 위해 QWERTY 방식이외의 방식이 제공되어야 한다.
- 국내 사용자를 위한 한글 기반 키패드를 제공해야 한다.
- 터치한 문자를 확인하면서 레코딩 공격에 강한 기법을 제공해야 한다.
- 문자를 손쉽게 입력할 수 있는 효율적인 방법이 필요하다.

II. 관련 연구

A. 가상 키패드

사용자는 인증을 위해 터치 스크린에 제공되는 가상 키패드를 이용하여 패스워드를 입력한다. 하지만 터치 스크린에 실수 없이 패스워드나 PIN을 입력해야 하지만 작은 크기의 제약을 가진다. 그림 1은 가상 키패드를 생성하는 방식으로 PC자판과 같은 배열을 가진 QWERTY 키패드와 알파벳 순서로 배치된 ABC 키패드 방식으로 구분[9,10].

기존 방식은 측면의 키패드가 고정되고, 그 이외의 키패드는 한 칸이나 두 칸 정도 떨어져 있어 터치한 위치가 노출되면 패스워드를 유추할 수 있다. 예를 들어, 사용자가 “asdfgh”을 터치하였을 때 공격자가 터치한 위치로 “asecgh”를 알아내었다면 패스워드 패턴을 통해 “ec” 대신에 “df”로 유추할 수 있다[7,9].

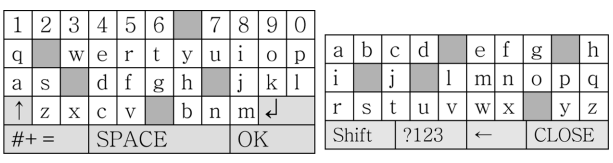


그림 1. QWERTY 키패드와 ABC 키패드

Fig. 1. QWERTY Keypads and ABC Keypads.

사용자가 패스워드를 입력하는 과정을 스마트 폰에 내장된 고해상도의 카메라를 이용하여 촬영하거나 어깨 너머로 훔쳐보는 것이 가능하다. 사용자의 입력 과정에서의 취약점을 해결하기 위한 연구가 진행되고 있다[3,11,12].

가상 키패드의 터치한 위치를 파악할 경우 패스워드가 노출될 가능성이 높고 이러한 취약점을 해결하기 위해 다양한 기법이 제시되고 있다.

- **물결형 보안 키패드(Ripple type)**는 QWERTY 키패드의 개선기법으로 각 열(colum)마다 반 칸의 공백을 추가하거나 각 열마다 키패드를 재배치하는 방식이다[10,11].
- **클론 키패드(clone)**는 QWERTY 키패드에서 한 줄을 추가형 복사하여 추가한다. 중복된 행으로 위치를 파악하기 어렵지만 키패드의 크기가 전체적으로 작아진다[12].
- **좌우 슬라이드 보안 키패드(touch & slide)**는 ABC 키패드를 개선하여 화살표를 터치하거나 슬라이드를 이용하여 좌우로 키패드를 이동하는 방식이다. PC자판에 익숙하지 않은 사용자에게 편리하지만 슬라이드로 원하는 문자를 찾아야 하는 불편함이 있다[12].

B. 개선된 보안 키패드

1) 시작 위치 랜덤 배치 보안 키패드

서화정의 보안 키패드는 그림 2와 같이 QWERTY 방식을 응용하되 시작 키패드를 임의의 위치에 배치하는 방식이다. 하지만 이 방식은 사용자가 “1”의 위치를 찾은 후, “1”을 기준으로 원하는 문자를 찾아가는 방식으로 QWERTY 자판을 외워야 하는 단점을 가진다[12,13].

2) 테트리스 모양 보안 키패드

기존 키패드는 직사각형으로 되어 있고 한 줄에 배치할 수 있는 공간이 제한되어 1~2칸의 여백만 가지기 때문에 취약점이 존재한다. 테트리스 보안 키패드는 그림 3과 같이 13가지의 테트리스 모양으로 키패드를 생성하여 배치하므로 여백의 공간을 많이 가질 수 있는 방식이다[12].

h	j	k	l	z	x	c	v	b		n
	m	1	2	3		4	5	6	7	8
9	0	q	w		e	r	t		y	u
↑	i	o	p	a	s	d	f	g	↲	
#+=			SPACE					OK		

그림 2. 서화정의 제안된 키패드

Fig. 2. Keypads proposed by Seo.

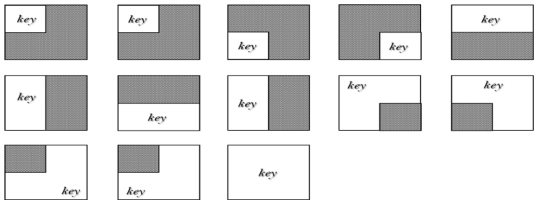


그림 3. 테트리스 모양의 키패드 종류

Fig. 3. Types of Tetris-shaped keypad.

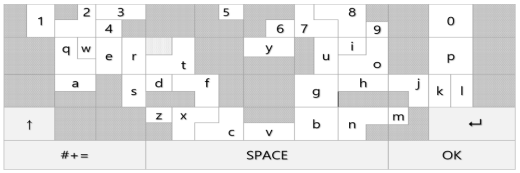


그림 4. 테트리스 보안 키패드의 예시

Fig. 4. Example of secure keypad with tetris type.

3/7	2/4	5/0
7/5	1/3	4/6
6/9	0/2	8/8
	9/1	OK

그림 5. 더블 터치를 가진 숫자 키패드

Fig. 5. Numeric keypad example with double touch

테트리스의 특성으로 인해 많은 여백을 확보하여 위치 기반 취약점에 강하다. 그림 4는 실제 적용된 보안 키패드의 사례이다.

3) 이중 터치 기반 숫자 보안 키패드

그림 5는 하나의 키패드에 2개의 숫자(n/M)가 표시되어 누르는 시간에 따라 다르게 입력할 수 있는 방식이다. 길게 터치하면 왼쪽 숫자가 입력되고, 1초 미만으로 누르면 오른쪽 숫자가 입력되는 방식이다. 같은 키패드를 통해 입력하기 때문에 훔쳐보기와 같은 공격이나 키로깅 공격(keylogging attack)으로부터 안전하지만 숫자 키패드에서만 적용가능하다는 단점이 있다[14].

C. 어깨 너머 공격을 회피 개선기법

사용자가 패스워드를 입력한 문자를 확인하기 위해 터치한 문자를 디스플레이 영역에 보여준다. 추가적으로 입력할 경우 마지막 문자만 보여주고, 나머지 이전에 문자는 ＊로 출력된다. 이 기능 때문에 몰래 촬영하거나 몰래 훔쳐볼 수 있다.

4색 정리(Four Color Theorem)은 평면을 여러 개의 영역으로 나누고 맞닿은 부분을 4개의 색으로 표시가 가능하다는 정리이다. 키패드를 4개의 색으로 표시한 후 디스플레이 영역에 색깔로 표시할 수 있다[15].

D. 그룹핑된 보안 키패드

1) 더블 터치 기반 보안 키패드

스마트 폰의 작은 스크린에 보여지는 문자의 개수를 줄이는 방법으로 입력 가능한 문자를 그룹으로 나누어 원하는 문자가 있는 그룹을 선택하고 그 다음에 원하는 문자를 입력하는 방식이다(그림 6). PC자판의 키패드를 기준으로 볼 때 10개의 숫자 26개의 영문자, 32개의 특수문자로 구성되어 있다.

그림 6은 그룹 키패드의 예시이고, (b)와 (c)처럼 숫자 그룹에서 터치할 때마다 배치순서를 변경할 수 있다.

그림 7은 그룹 목록을 보여주고, 그룹을 선택하는 과정이다. (b)는 GP#1인 숫자그룹을 선택한 경우이고 (c)는 영문(모음) 그룹을 선택한 모습이다. 패스워드가 7 9이면 처음 화면(a)에서 GP#1를 선택하고 다음 단계(b)에서 7을 터치하고 그

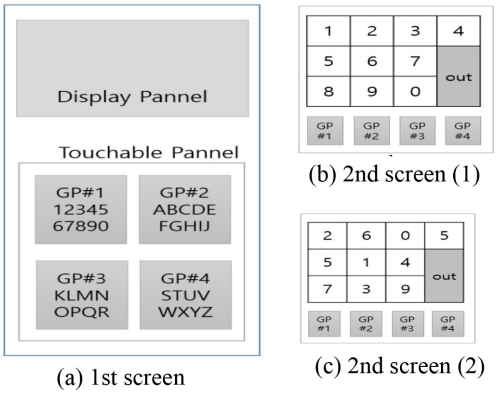


그림 6. 그룹 키패드의 예시

Fig. 6. Examples of Group Keypads. (a)1st step (b) 2nd step (c) 2nd* step.

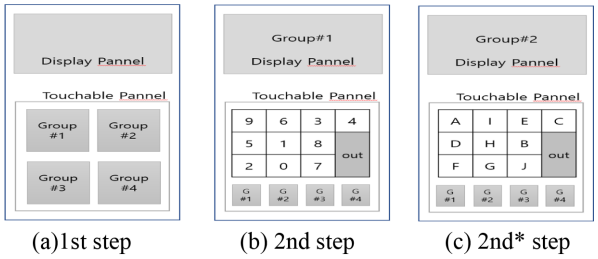


그림 7. 패스워드 입력 과정

Fig. 7. Password input process.

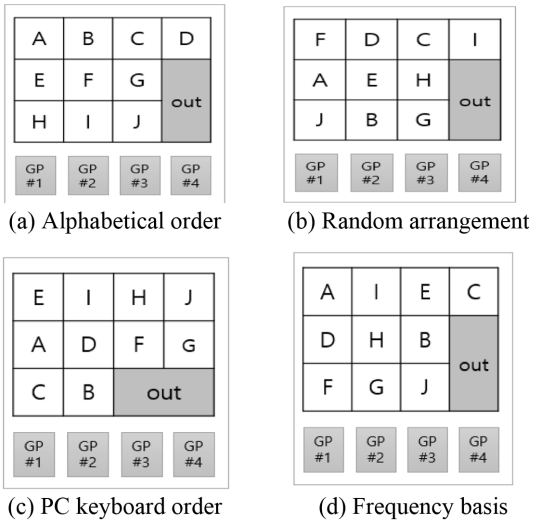


그림 8. 2단계에서 키패드 배치 방법

Fig. 8. Method of Keypad Generated in the 2nd stage.

다음 키패드가 같은 그룹이라 바로 9를 터치한다. 다른 그룹에 있는 경우 첫화면(out 버튼 이용)으로 이동하거나 하단의 그룹을 선택하여 들어가 원하는 문자를 터치하여 입력한다.

2) 그룹 키패드 배치기법

각 키패드의 배치 순서를 변경하여 취약점을 극복할 수 있다. 그림 8과 같이 그룹 내의 키패드(“ABCDEFGHIJ”)를 다양하게 배치할 수 있다[3].

- 오름차순으로 배치하는 방법(그림 8(a)).
- 터치할 때마다 랜덤하게 배치하는 방법(그림 8(b)).
- PC자판과 같은 방식으로 배치하는 방법(그림 8(c)).
- 빈도수가 높은 문자 순서대로 배치하는 방법(그림 8(d)).

III. 개선된 그룹 키패드 기법

A. 그룹화된 키패드 기존 연구

그룹화된 키패드에 대한 기법들이 그룹을 선택하는 방식이 아닌 첫화면에서 직접 보여주는 방식으로 제안되었다[16]. 그림 9는 그룹화된 키패드를 테두리에 제시하고 중앙 영역에 터치할 키패드를 보여준다. 왼쪽은 터치하는 키패드 영역을 표시한 것이고, 오른쪽 “qwert” 그룹을 선택했을 때 모습이다. 그룹 키패드는 그룹별로 키패드를 첫 화면에 제시하였지만 보여지는 키패드의 크기가 작고 사용 편의성이 부족하다.

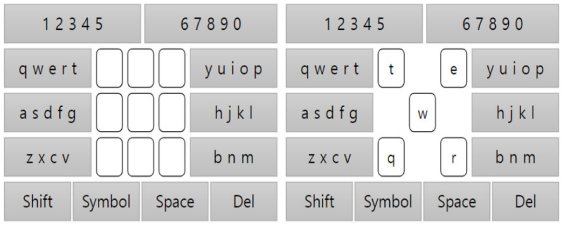


그림 9. 그룹화된 키패드

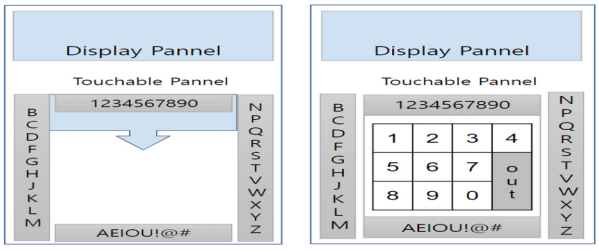
Fig. 9. Keypad with grouped keys.

B. 안전성을 고려한 개선된 제안 기법

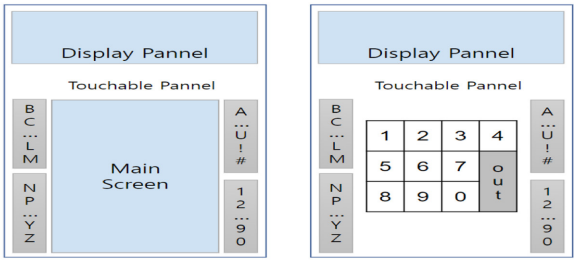
제안 기법은 사용자의 편의성을 보장하기 위해 첫화면에서 그룹을 선택하는 그룹 키패드의 방식을 제시하고 있다.

- PC자판 형태의 QWERTY 방식
- ABC 순 배치 방식 : 그룹을 생성할 때 모음과 자음 2개의 그룹으로 나눌 수 있다. 영어 사전에서 빈도수에 따라 4개의 그룹으로 나눌 수도 있다. 즉, G#1-EARIOT G#2-NSLCUD G#3-PMHGBF G#4-YWKVXZJQ와 같이 나눌 수 있다. 마지막 그룹은 빈도수가 낮아서 8개 문자로 구성하였다.
- 국내 사용자의 한글 병기 키패드 방식 : 국내에서는 패스워드를 생성할 때 영문으로 된 문자보다는 PC자판에 있는 키패드의 한글의 자음과 모음으로 생성하는 경우가 많다. 즉, 홍길동은 이름으로 패스워드를 만든다면 "honggildong"이 아닌 "ghdrlfehd"이다. 이때 사용자는 패스워드를 한글 자판의 홍길동으로 외우지 영문 자판의 영문자로 외우지 않기 때문에 입력에 어려움이 있다. 제안한 기법은 그룹을 생성하여 제시하기 때문에 국내 사용자의 패스워드 생성 기법을 기반으로 인한 문제를 해결할 수 있다.

그림 10은 ABC 방식에서 숫자 그룹을 선택하였을 때의 화면이다. 그림 10(a)는 그룹이 상하좌우로 배치된 모습이며, 숫자 그룹를 드래그하여 그룹을 선택한 모습이다. 그림 10(b)는 그룹이 좌우로 배치된 경우로 스마트 폰의 세로 화면에 적합한 모습이다.



(a) 상하좌우로 배치



(b) 좌우로 배치

그림 10. ABC 방식으로 숫자 그룹을 선택한 경우

Fig. 10. Cases of Selecting Number Groups in ABC Method.

IV. 제안 기법의 동작과정 및 분석

A. 보안 키패드 배치 및 효율적 입력 방법

첫화면에서 그룹 선택한 후, 10~12개 그룹내 키패드는 메인 영역에 배치한다. 기존 그룹 키패드와 마찬가지로 배치 순서를 변경하므로 취약점을 극복할 수 있다[3,16].

기존 방식은 해당 키패드를 터치하는 방식이지만 제안 기법에서는 스마트 폰의 특성을 고려하여 드래그를 적절하게 이용하여 입력할 수 있다. "abhi"를 입력할 경우 기존 방식처럼 a, b, h, i순으로 터치하는 방법과 "a,b,h"를 그림 11과 같이 드래그하고 떨어져 있는 키패드 "i"를 터치할 수 있다.

만약에 "abhii"를 입력하는 경우 i를 두 번 터치하면 패스워드를 쉽게 입력할 수 있다. 제안기법은 12개의 문자 키패드를 표시되지만 숫자처럼 10개의 키패드가 보여질 경우 그림 12와 같이 다양한 모양으로 구성할 수 있다. 잘 보이지 않는 영역이나 자주 사용하는 키패드는 직사각형의 형태로 제시한다.

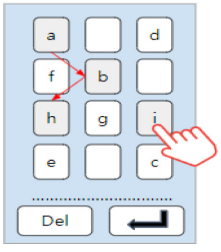


그림 11. 드래그를 이용한 패스워드 입력 방법

Fig. 11. Password Input Method Using Drag.

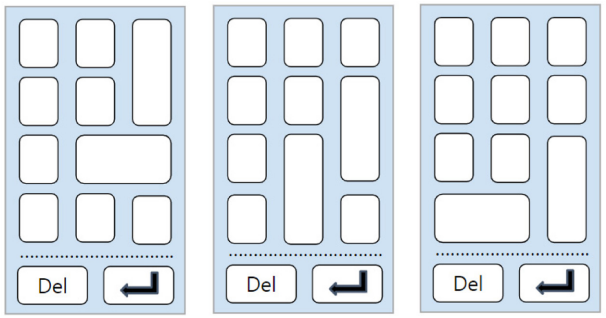


그림 12. 다양한 형태의 키패드 배치
Fig. 12. Various Keypad Layouts.

B. 레코딩 공격에 강한 제안 기법

입력된 패스워드가 디스플레이에 보여진다. 구글 글래스나 스마트 폰을 이용한 카메라로 패스워드를 터치하는 과정을 녹화하여 사용자의 패스워드를 알아낼 수 있다. 그림 13의 왼쪽 그림과 같이 사용자가 패스워드를 터치할 때마다 디스플레이에 마지막 문자가 보여진다. 제안한 기법에서는 하나의 그룹이 9~10개 정도의 키패드를 가지고 있고, 이 키패드를 중앙에 배치한다. 중앙에 12개의 키패드를 배치할 수 있는 영역이다. 그림 13의 오른쪽 그림과 같이 키패드를 출력할 때 각각의 키패드에 색상이나 아이콘 형태 등의 추가적인 정보를 제공한다.

색상이 반영된 경우 터치한 키패드의 색을 디스플레이에 표시하여 터치 오류를 바로 확인할 수 있다. 사용자의 터치한 영역을 가린다면 레코딩 공격을 차단할 수 있다.

제안한 기법에서는 터치할 때마다 키패드 모양을 보여주므로 입력하는 과정을 스마트 폰 정면에서 바로 보지 않고서는 사용자가 입력한 키패드를 확인할 수 없다.

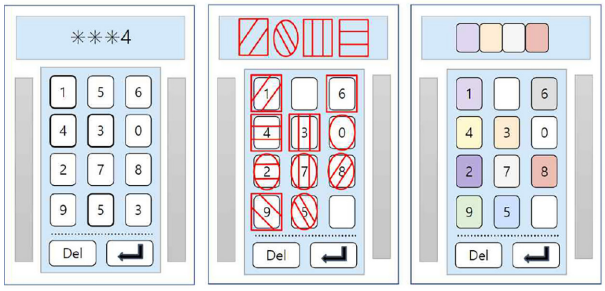


그림 13. 입력한 키패드 모양 출력
Fig. 13. Display of the Entered Keypad Shape.

C. 기존 기법과의 비교분석 및 평가

디스플레이가 작은 스마트 폰에서 키패드는 쉽게 찾을 수 있고, 위치 취약점에 대응하고, 훔쳐보기 등의 공격을 차단할 필요가 있다. 제안 기법은 그룹 선택 방법과 그룹핑 방법, 키패드를 터치하는 방법, 입력한 패스워드 확인 방법 등에서 개선된 방법을 제시하고 있다. 이를 통해 서론에서 제시된 요구사항을 만족하고 있다.

- 기존 보안 키패드의 근본적인 문제인 키패드의 크기이다. 그룹 키패드는 그룹 선택 후 보여지는 문자의 개수가 10개 이하라 크기 조절이 가능하다. 또한 다양한 키패드 배치로 터치한 위치 취약점을 최소화하면서 쉽게 찾을 수 있다.
- 기존의 그룹 키패드의 문제점이 그룹 선택후 내부 키패드를 터치하는 번거러움이 존재하였지만 제안 기법에서는 그룹핑 키패드 모음을 측면에 배치하여 필요한 그룹을 선택하는 방식으로 번거러움을 최소화하고 있다.
- 제안 기법은 첫화면에서 사용자가 QWERTY 방식이나 ABC 방식 등의 입력방식을 선택할 수 있다.
- 국내 사용자의 한글로 패스워드를 만드는 경우가 빈번하다. 하지만 기존 키패드는 영문자와 한글의 자·모음이 병기되지 않아 외워야 하는 번거러움이 존재한다. 제안 기법에서는 첫화면에서 영문자와 한글병기한 방식을 선택할 수 있다.
- 제안 기법은 마지막 문자를 확인하는 대신에 키패드마다 색깔이나 모양을 추가적으로 표시하여 터치한 문자를 확인할 수 있어 레코딩 공격에 강인하다.
- 제안 기법에서는 드래그 기능을 추가하여 이어서 터치가 가능할 경우 그림 11과 같이 드래그해서 입력하고 더 이상 잇기 어려울 경우 다시 원하는 문자를 터치하는 방식으로 입력에 효율성을 추가하였다.

모든 문자가 보여지는 기존 방식보다 터치횟수가 늘어나는 단점이 있지만 제안 기법에서 그룹을 터치하거나 드래그하여 선택한 후 패스워드를 입력하기 때문에 기존 그룹 키패드보다는 사용에 대한 편의성을 가진다.

V. 결 론

핀테크 환경에서 스마트 폰을 이용한 안전한 패스워드 입력에 대한 필요성이 제기되고 있다. 사용자 인증을 위해 패스워드의 안전한 입력이 요구된다.

스마트 폰으로 패스워드 입력에 대한 취약점을 해결하기 위한 다양한 연구가 진행되고 있다. 스마트 폰의 패스워드 취약점을 해결하기 위한 방법으로 그룹 키패드가 제안되었지만 사용의 편의성이 부족하여 이를 개선하는 기법을 제안하였다.

제안 기법에서는 그룹의 배치, 효율적인 입력방법, 그룹내의 10개 이내의 키패드 배치방법 등을 제시하여 효율성과 편의성을 제공하였다.

향후에는 본 논문에서 제안한 개선된 그룹 키패드의 설계를 실제로 구현하여 사용자의 경험을 통한 편리성과 안전성에 대한 분석이 요구된다.

참고문헌

[1] J. H. Jeon, "A study on the security vulnerability factors of smart phones," *Jouranl of Information and Security*, vol. 22, no. 2, pp. 43-50, 2022.

[2] C. Nayak, M. Parhi, and S. Ghosal, "Robust virtual keyboard for online banking," *International Journal of Computer Applications*, vol. 107, no. 21, pp. 36-38, 2014. doi: 10.5120/19142-0530

[3] H. J. Mun, "Design for position protection secure keypads based on double-touch using grouping in the fintech," *Journal of Convergence for Information Technology,* vol. 12, no. 3, pp. 38-45, 2022. doi: 10.22156/CS4SMB.2022.12.03.038

[4] J. O. Park and B. W. Jin, "A study on authentication method for secure payment in fintech environment," *The Journal of the Institute of Internet, Broadcasting and Communication,* vol. 15, no. 4, pp. 25-31, 2015.

[5] D. Y. Kim and S. M. Cho, "A proposal of smart phone app for preventing smishing attack," *Journal of Security Engineering,* vol. 12, no. 3, pp. 207-220, 2015.

[6] S. H. Kim, M. S. Park, and S. J. Kim, "Shoulder surfing attack modeling and security analysis on commercial keypad schemes," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 24, no. 6, pp. 1159-1174, 2014. doi: 10.13089/JKIISC.2014.24.6.1159

[7] G. O. Baik, C. H. Lim, and J. G. Shon, "A virtual keyboard system for preventing keylogging," *Journal of Security Engineering*, vol. 7, no. 4, pp. 319-334, 2010.

[8] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My google glass sees your passwords!," *Proceedings of the Black Hat USA*, 2014.

[9] J. S. Song, M. W. Chung, S. H. Seo, and S. H. Lee, "Security vulnerability analysis of simple mobile payments services," *The Korea Information Processing Society Fall Conference*, vol. 22, no. 2, pp. 817-820, 2015.

[10] D. H. Lee, D. H. Bae, S. L. Yoo, J. Y. Chae, Y. Lee, and H. G. Yang, "Analysis of safety in secure keypads for smartphone," *REVIEW of the Korea Institute of Information Security and Cryptology*, vol. 21, no. 7, pp. 30-37, 2011. doi: KIISC.2011.21.7.30

[11] W. G. Pak, S. Yeo, and Y. R. Cha, "A secure virtual keypad for mobile devices," *Proceeding of Korea Information Science Society,* pp. 875-876, 2015.

[12] H. J. Mun, "Virtual keypads based on tetris with resistance for attack using location information," *Journal of the Korea Convergence Society,* vol. 8, no. 6, pp. 37-44, 2017. doi: 10.15207/JKCS.2017.8.6.037

[13] Y. H. Lee, "An analysis on the vulnerability of secure keypads for mobile devices," *Journal of Korean Society for Internet Information*, vol. 14, no. 3, pp. 15-21, 2013.

[14] J. Song, M. W. Jung, J. I. Choi, and S. H. Seo, "Proposal and implementation of security keypad with dual touch," *KIPS Transactions on Computer and Communication Systems,* vol. 7, no. 3, pp. 73-80, 2018. doi: 10.3745/KTCCS.2018.7.3.73

[15] H. J. Kim, H. J. Seo, Y. C. Lee, T. H. Park, and H. W. Kim, "Implementation of virtual finace keypads with resistance for shoulder surfing attack," *REVIEW the Korea Institute of Information Security and Cryptology(KIISC)*, vol. 23, no. 6, pp. 21-29, 2013. https://koreascience.kr/article/JAKO201304163995554.page

[16] I. Kim, "Secure numeric keypad against attacks guessing passwords from key touching," *Journal of Knowledge Information Technology and Systems*, vol. 15, no. 5, pp. 591-598, 2020. doi: 10.34163/jkits.2020.15.5.001

문 형 진 (Hyung-Jin Mun)_종신회원

1996년 2월 : 충남대학교 수학과 졸업
2008년 2월 : 충북대학교 전자계산학(이학박사)
2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
2017년 3월 ~ 현재 : 성결대학교 정보통신공학과 조교수
〈관심분야〉 정보보호, 네트워크 보안, Fintech 보안, 사용자인증